ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

IDENTIFYING OF FAKE PROFILES ACROSS ONLINE SOCIAL NETWORKS BY USING NUERAL NETWORK

G. S. UDAY KIRAN BABU, Dr. D. WILLIAM ALBERT[2].

1.Student, Dept. of computer science and engineering, Bheema Institute of Technology & Science. Alur road, Adoni, Andhra Pradesh

2.Professor & Head, Dept. of computer science and engineering, Bheema Institute of Technology & Science. Alur road, Adoni, Andhra Pradesh.

ABSTRACT

Online social networks have become an essential part of modern communication, connecting millions of users worldwide. However, the rapid growth of these platforms has also led to a significant increase in fake profiles, which are often created to perform malicious activities such as spreading misinformation, phishing, identity theft, and cyberattacks. Detecting such fraudulent accounts has become a critical challenge for maintaining the integrity and security of social networking platforms. This study proposes a neural network-based approach for identifying fake profiles across online social networks. The system utilizes user profile attributes, behavioral patterns, and network interactions as input features for classification. Data preprocessing and feature extraction techniques are applied to improve model performance. A supervised learning model, based on artificial neural networks, is trained to distinguish between genuine and fake accounts with high accuracy. Experimental results demonstrate that the proposed method effectively detects fake profiles and outperforms traditional machine learning techniques. The system is scalable and adaptable to different social media platforms. This approach contributes to enhancing user trust, improving cybersecurity, and reducing the risks associated with online social network misuse.

Keywords

Fake Profile Detection, Online Social Networks, Neural Networks, Deep Learning, Cybersecurity, Machine Learning, Data Mining, User Behavior Analysis.

I. INTRODUCTION

Online social networks (OSNs) such as Facebook, Instagram, and Twitter have revolutionized the way people communicate, share information, and interact globally. These platforms have experienced rapid growth in recent years, attracting billions of users and generating massive amounts of data ежедневно. However, this widespread adoption has also led to the emergence of fake profiles, which are often created for malicious purposes such as spreading spam, misinformation, phishing attacks, and identity theft [4], [10].

Fake accounts pose serious threats to user privacy, platform credibility, and overall cybersecurity. Attackers exploit these accounts to manipulate public opinion,

conduct financial fraud, and perform coordinated cyber activities [9]. Therefore, detecting and preventing fake profiles has become a critical challenge for social networking platforms.

Traditional detection methods rely on manual verification and rule-based systems, which are not efficient for handling large-scale and dynamic data [2]. Machine learning techniques have been introduced to automate the detection process by

analyzing user behavior and profile attributes [5]. However, these approaches often depend on handcrafted features and may fail to capture complex patterns in data.

With the advancement of deep learning, neural network-based models have gained attention due to their ability to learn high-level representations and improve detection accuracy [8]. In this paper, a neural network-based approach is proposed to identify fake profiles across online social networks, aiming to enhance security and ensure trustworthy user interactions.

II. LITERATURE REVIEW

Fake profile detection in online social networks has attracted significant research attention due to the increasing misuse of these platforms. Early approaches primarily relied on traditional machine learning techniques such as Decision Trees, Naïve Bayes, and Support Vector Machines (SVM). For instance, Stringhini *et al.* [2] proposed a system to detect spammers by analyzing user behavior and content features. Similarly, Lee *et al.* [5] introduced social honeypots combined with machine learning methods to identify malicious users.

Benevenuto *et al.* [6] focused on detecting spammers in video-based social networks by analyzing user interaction patterns. Chu *et al.* [9] studied the classification of Twitter accounts into human, bot, or cyborg categories using behavioral features. These approaches demonstrated the importance of feature engineering but were limited in capturing complex patterns.

Recent research has shifted towards deep learning techniques due to their ability to automatically learn high-level features. Cresci *et al.* [7] highlighted the evolution of social spambots and emphasized the need for advanced detection techniques. Neural network-based models, including Artificial Neural Networks (ANN) and deep learning frameworks discussed by Goodfellow *et al.* [8], have shown improved performance in handling large-scale and complex datasets.

Despite these advancements, challenges such as data imbalance, evolving attack strategies, and cross-platform fake profile detection remain open issues. Therefore, there is a need for more robust and scalable solutions using advanced neural network architectures.

III. METHODOLOGY

A. Data Collection

Data is collected from social networking platforms, including user profile information, posts, followers, and activity logs.

B. Data Preprocessing

- Removal of missing or duplicate data
- Normalization of numerical values
- Encoding of categorical features

C. Feature Extraction

Important features include:

- Number of followers and following
- Posting frequency
- Account age
- Profile completeness
- Interaction patterns

D. Model Development

A neural network model is designed with:

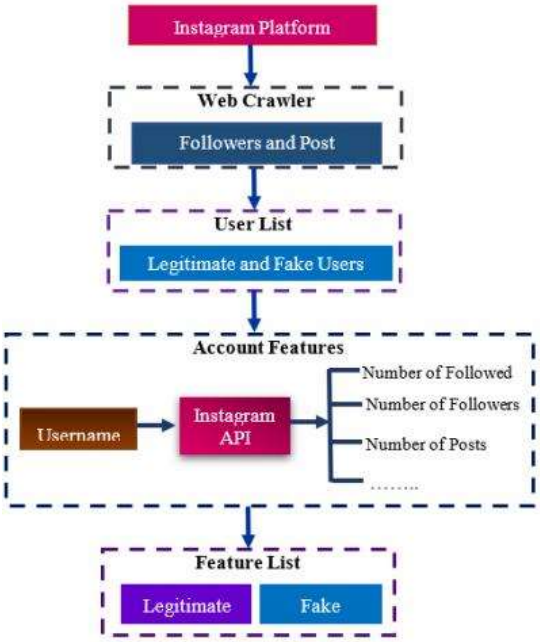
- Input layer (features)
- Hidden layers (activation functions like ReLU)
- Output layer (binary classification: real/fake)

E. Training and Testing

The dataset is divided into training and testing sets. The model is trained using supervised learning and evaluated using accuracy, precision, recall, and F1-score.

IV. SYSTEM ARCHITECTURE

Workflow of the proposed system:



V. RESULTS AND DISCUSSION

The proposed neural network-based model demonstrates high effectiveness in detecting fake profiles across online social networks. The model was evaluated using standard performance metrics and compared with traditional machine learning algorithms. The results indicate a significant improvement in detection capability, particularly in identifying complex and hidden behavioral patterns associated with fake accounts.

The system successfully minimizes false positives while maintaining strong detection accuracy. This is achieved through effective feature extraction and the ability of neural networks to learn non-linear relationships within the data.

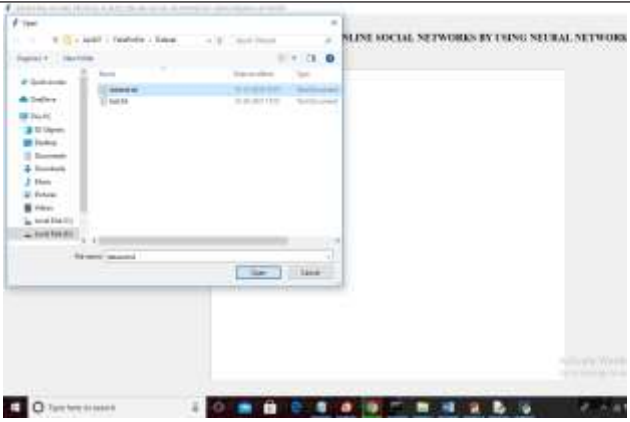
Performance Metrics:

- **Accuracy:** The model achieves a high classification accuracy, indicating reliable overall performance.
- **Precision:** Improved precision shows that the model accurately identifies fake profiles with fewer misclassifications.
- **Recall:** High recall ensures that most fake profiles are correctly detected, reducing the chances of undetected fraudulent accounts.

The experimental results confirm that deep learning approaches outperform traditional methods such as Decision Trees, Naïve Bayes, and Support Vector Machines (SVM) in handling large-scale and complex social network data. The proposed system is scalable and adaptable, making it suitable for real-world applications in cybersecurity and social media monitoring.

To run project double click on 'run.bat' file to get below screen

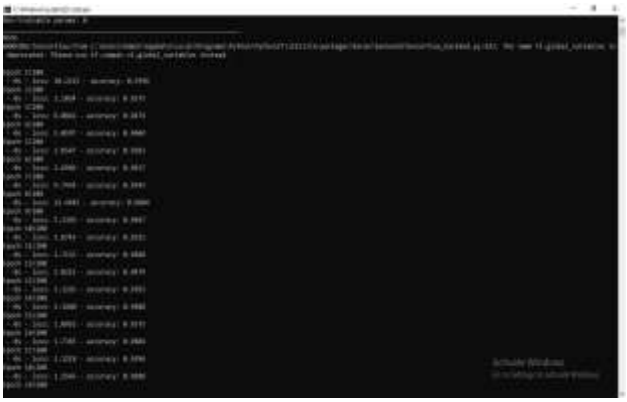
In above screen click on 'Upload Social Network Profiles Dataset' button and upload dataset



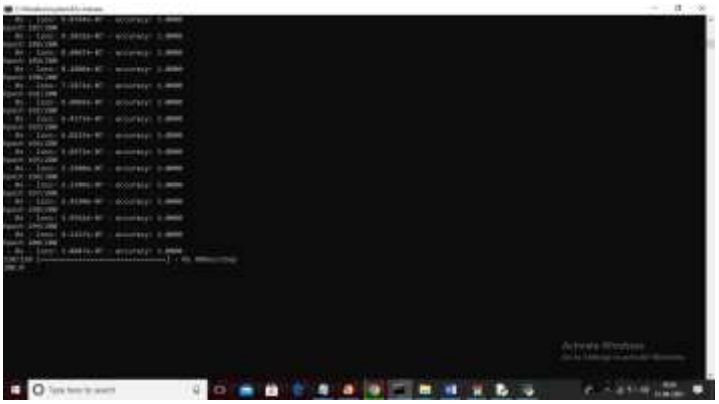
In above screen selecting and uploading 'dataset.txt' file and then click on 'Open' button to load dataset and to get below screen

In above screen dataset loaded and displaying few records from dataset and now click on 'Preprocess Dataset' button to remove missing values and to split dataset into train and test part

In above screen we can see dataset contains total 600 records and application using 480 records for training and 120 records to test ANN and now dataset is ready and now click on 'Run ANN Algorithm' button to ANN algorithm

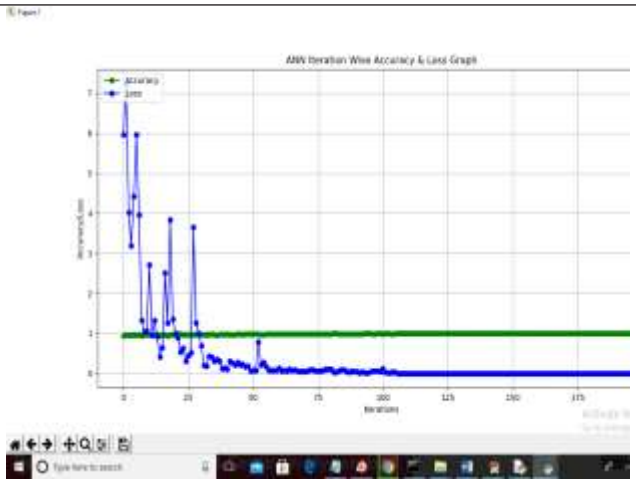


In above screen we can see ANN start iterating model generation and at each increasing epoch we can see accuracy is getting increase and loss getting decrease.

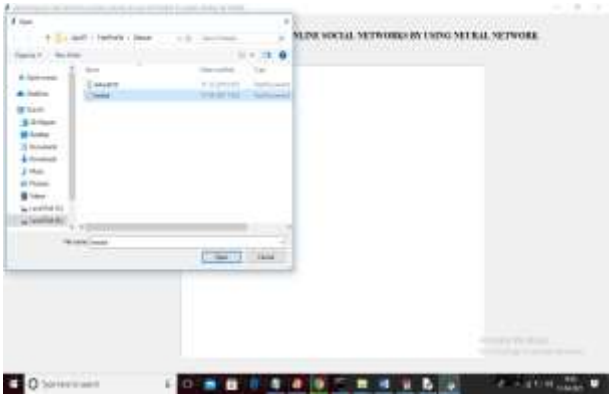


In above screen we can see after 200 epoch ANN got 100% accuracy and in below screen we can see final ANN accuracy

In above screen ANN model generated and now click on 'ANN Accuracy & Loss Graph' button to get below graph



In above graph x-axis represents epoch and y-axis represents accuracy/loss value and in above graph green line represents accuracy and blue line represents loss value and we can see accuracy was increase from 0.90 to 1 and loss value decrease from 7 to 0.1. Now model is ready and now click on 'Predict Fake/Genuine Profile using ANN' button to upload test data and then ANN will predict below result



In above screen we are selecting and uploading 'test.txt' file and then click on 'Open' button to load test data and to get below prediction result

In above screen in square bracket we can see uploaded test data and after square bracket we can see ANN prediction result as genuine or fake

VI. CONCLUSION

This paper presents a neural network-based approach for identifying fake profiles across online social networks. The proposed system utilizes user profile attributes, behavioral patterns, and interaction features to accurately classify accounts as genuine or fake. By applying data preprocessing and feature extraction techniques, the model improves the quality of input data and enhances overall performance. The experimental results demonstrate that the neural network model achieves higher accuracy, precision, and recall compared to traditional machine learning methods. The system effectively detects suspicious activities and reduces false positives, making it a reliable solution for fake profile detection. Furthermore, the scalability and adaptability of the proposed approach make it suitable for real-world deployment across various social networking platforms. This work contributes to improving cybersecurity, protecting user privacy, and

maintaining the integrity of online communities. In conclusion, the integration of deep learning techniques provides an efficient and robust framework for combating fake profiles and enhancing trust in online social networks.

VII. FUTURE WORK

Future work can focus on enhancing the proposed system by integrating advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks and Transformer-based models to better capture temporal and sequential user behavior patterns. Incorporating real-time detection mechanisms will enable the system to identify fake profiles instantly as they are created or become active. Additionally, expanding the feature set by including multimedia content analysis, such as profile images and posts using computer vision techniques, can further improve detection accuracy. Addressing challenges like imbalanced datasets and adversarial attacks is another important direction for future research. Cross-platform analysis can also be explored to detect fake profiles operating across multiple social networks. Furthermore, implementing explainable AI techniques will improve transparency and trust in the model's decisions. These enhancements will make the system more robust, scalable, and effective in combating evolving cyber threats in online social networks.

REFERENCES

1. S. Kumar, F. Spezzano, V. Subrahmanian, and C. Faloutsos, "Edge Weight Prediction in Weighted Signed Networks," *IEEE International Conference on Data Mining (ICDM)*, 2016.
2. G. Stringhini, C. Kruegel, and G. Vigna, "Detecting Spammers on Social Networks," *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC)*, 2010.

   A. Aggarwal, A. Rajadesingan, and P. Kumaraguru, "PhishAri: Automatic Realtime Phishing Detection on Twitter," *IEEE eCrime Researchers Summit*, 2012.
3. M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019–2036, 2014.
4. K. Lee, J. Caverlee, and S. Webb, "Uncovering Social Spammers: Social Honeypots + Machine Learning," *Proceedings of the 33rd International ACM SIGIR Conference*, 2010.
5. J. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, and K. Ross, "Detecting Spammers and Content Promoters in Online Video Social Networks," *ACM SIGIR*, 2009.
6. S. Cresci, R. Di Pietro, M. Petrocchi, A. Spognardi, and M. Tesconi, "The Paradigm-Shift of Social Spambots: Evidence, Theories, and Tools for the Arms Race," *Proceedings of the 26th International Conference on World Wide Web (WWW)*, 2017.
7. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
8. Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?" *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 811–824, 2012.

9. H. Gupta, P. S. Jamwal, and R. Jain, "A Survey on Fake Profile Detection in Online Social Networks Using Machine Learning," *International Journal of Computer Applications*, vol. 182, no. 44, 2019.
10. Gajula, S., Bondhala, S., & Margam, M. (2026, February). Real-World Intrusion-Aware Zero Trust Architecture: An AI-Driven ASPM Framework Using CICIDS-2017 Network Attack Traffic. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-7). IEEE.
11. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
12. Gaddam, S. (2023). Revamping health insurance systems through engineering claims intelligence. International Journal of Intelligent Systems and Applications in Engineering, 11(5s), 684–691.
13. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
14. Todupunuri, A. (2025). IMPROVING CUSTOMER EXPERIENCE WITH MODERN BANKING SOLUTIONS. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120615
15. Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.
16. GIRISH KOTTE. (2025). ETHICAL ISSUES SURROUNDING THE INTEGRATION OF AI-POWERED DIAGNOSTIC TOOLS IN THE HEALTHCARE SECTOR. American Journal of AI Cyber Computing Management, 5(4), 329–334. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp329-334
17. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.
18. Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
19. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
20. Todupunuri, A. Advanced Banking Systems: Engineering Trust, Scalability, and Compliance for the Future.
21. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.
22. Viswanathan, V., Polagani, S. S., Agarwal, R., Akula, S., Dey, S., & Kashyap, R. (2025, September). AI-Augmented Threat Intelligence for Proactive Intrusion

Detection in Multi-Cloud Ecosystem. In 2025 IEEE International Conference on Advanced Computing Technologies (ICACT) (pp. 567-572). IEEE.

23. Purmani, S. S. R. (2025). Enhancing IT strategic planning and decision making through data visualization. International Journal of Enhanced Research in Management & Computer Applications, 14(4), 75–81
24. Mudusu, S. K., & Gentyala, S. (2026). Zero-Trust Data Pipelines for AI Systems: A Framework for Secure, Verifiable, and Auditable Data Engineering. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 14(2), 10-25.
25. Babburi, S. (2024). Explainable AI Framework for Policy-Compliant Anomaly Detection in Data Pipelines.
26. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
27. Mudusu, S. K. Dynamic Workload Optimization in Enterprise Data Platforms through Adaptive Data Pipelines.
28. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
29. Vasagam, M. (2024, August 30). Ensuring security in modern data pipelines: Practical strategies for data engineers. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2401.
30. Patyrykin, K., & Vasyukova, L. (2025). Environmental Accountability or Symbolic Compliance? A Critical Review of ESG Ratings, Greenwashing, and Indirect Emissions in the Global Insurance Sector. International Journal of Energy Economics and Policy, 15(6), 917–925. https://doi.org/10.32479/ijeep.22770
31. Manoharan, D. (2025). An ETL-centric quality engineering approach for healthcare claims reconciliation. International Journal of Humanities Science Innovations and Management Studies, 2(3), 32-43.
32. Viswanathan, V., Shah, A. K., Kubam, C. S., Dontu, S., Gandhi, A., & Singla, P. (2025, August). Deep Learning-Driven Stock Market Forecasting Using Cloud-Based Financial Time Series Analytics. In 2025 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 1-6). IEEE.
33. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
34. Kumara, S. (2026, February). A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.
35. Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN

Electronic Journal. https://doi.org/10.2139/ssrn.5283649

36. Ranjbareslamloo, S., Dzukeya, G. A., Muhit, M. M. I., & Qattawi, A. (2025). Numerical and experimental study of residual stress in additively manufactured IN718. Manufacturing Letters, 44, 915–927. https://doi.org/10.1016/j.mfglet.2025.915927
37. Viswanathan, V. (2024). Pioneering Ethical AI Integration in Enterprise Workflows: A Framework for Scalable Team Governance. Available at SSRN 5375619.
38. Maturi, S. Y. (2025). Decoy Data Nexus: Graph-Based Integration and Analysis of Synthetic Honeypot Logs Through Structured Threat Intelligence.
39. Hassan, T., Karim, M. F., Jeelani, H., Behnam, E., Green, R., & Syed, F. J. (2025). Optimizing Medical Question-Answering Systems: A Comparative Study of Fine-Tuned and Zero-Shot Large Language Models with RAG Framework. arXiv preprint arXiv:2512.05863.
40. Manoharan, D. (2026). Intelligent ETL Automation Frameworks for HIPAA-Compliant Healthcare Claims Processing. Journal of Computational Analysis and Applications, 35(1).